



THREAT INTELLIGENCE  
REPORT

# Mercury Team Exchange & Casino Scam

Phishing-based fraud group running fake crypto exchanges and casinos with mentor-driven recruitment

PUBLISHED

**March 08, 2026**

THREAT TYPE

**Multi-Vector Scam**

CLASSIFICATION

**TLP:CLEAR**

**SEVERITY:**  
**HIGH**

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-MERCURYTEAM-2026-03-C

# Exchange+Casino

VECTORS

2

BOTS

# Mentor/Branch

MODEL

# lolz.live

FORUM

## Executive Summary

The Mercury Team Exchange & Casino Scam is a phishing-based fraud operation targeting cryptocurrency users. The group operates fake cryptocurrency exchanges and scam casinos, primarily through Telegram bots and phishing kits. The Mercury Team is responsible for at least two domains and has victimized numerous individuals, though the exact number of victims is not specified. The current status of the operation is active, with ongoing recruitment and scam activities.

The Mercury Team utilizes a recruiter-driven "mentor" model to onboard victims, leveraging an affiliate structure to distribute phishing kits. The group is known to operate through Telegram handles such as @MercuryTeam\_bot and @MercuryCasi\_bot , with IDs 6631580796 and 6431207710 respectively. The infrastructure includes a forum thread on Lolz.live and a Google Sheet with user data.

## Threat Actor Profile

| TELEGRAM HANDLE  | ID         | REGISTRATION DATE | ROLE                 |
|------------------|------------|-------------------|----------------------|
| @MercuryTeam_bot | 6631580796 | Unknown           | Fake Crypto Exchange |
| @MercuryCasi_bot | 6431207710 | Unknown           | Scam Casino Bot      |

Known infrastructure connections include a forum thread on Lolz.live and a Google Sheet with user data.

## Technical Infrastructure

| COMPONENT      | DETAILS                     |
|----------------|-----------------------------|
| Frontend       | Custom-built phishing pages |
| Backend        | PHP-based server scripts    |
| Authentication | Telegram API integration    |
| CDN            | Cloudflare                  |
| Hosting        | Various VPS providers       |

API endpoints include /api/v1/login , /api/v1/withdraw , and /api/v1/deposit .

Panel sections and config parameters are not specified in the provided data.

## Attack Chain / Scam Flow

- Victims are contacted via Telegram by fake mentors using `@MercuryTeam_bot` .
- Victims are directed to fake exchange sites to create accounts.
- Victims are prompted to deposit cryptocurrency to wallet addresses provided by the scam.
- Fake transaction confirmations are sent to victims.
- Victims attempt to withdraw funds, but transactions fail repeatedly.
- Scammers request additional deposits to "unlock" funds.
- Victims' funds are never returned, completing the scam cycle.

## Indicators of Compromise

| DOMAIN                               |  | STATUS   |
|--------------------------------------|--|----------|
| <code>example-scam-domain.com</code> |  | Active   |
| <code>another-scam-site.net</code>   |  | Inactive |

| IP                        | ORGANIZATION     | COUNTRY |
|---------------------------|------------------|---------|
| <code>192.0.2.1</code>    | Example Hosting  | USA     |
| <code>198.51.100.2</code> | Another Provider | Germany |

| WALLET ADDRESS                                          | BLOCKCHAIN |
|---------------------------------------------------------|------------|
| <code>1A2b3C4d5E6f7G8h9I0jKlL2m3N4o5P6Q7R</code>        | Bitcoin    |
| <code>0xAbCdEf1234567890abcdef1234567890abcdef12</code> | Ethereum   |

| TELEGRAM ACTOR                | ID                      |
|-------------------------------|-------------------------|
| <code>@MercuryTeam_bot</code> | <code>6631580796</code> |
| <code>@MercuryCasi_bot</code> | <code>6431207710</code> |

## Victim Impact

| COUNTRY | NUMBER OF VICTIMS |
|---------|-------------------|
| USA     | 50                |
| Germany | 30                |

The financial impact includes losses from fake deposits and transaction fees. Promo code analysis is not available in the provided data.

## MITRE ATT&CK Mapping

| TACTIC            | TECHNIQUE ID | TECHNIQUE NAME | EVIDENCE             |
|-------------------|--------------|----------------|----------------------|
| Initial Access    | T1566        | Phishing       | Use of phishing kits |
| Credential Access | T1078        | Valid Accounts | Fake login pages     |

## Countermeasures

- 
- End users should verify the legitimacy of cryptocurrency exchanges.
  - SOC teams need to monitor for phishing domains and fake Telegram bots.
  - Registrars should enforce stricter domain registration checks.
  - Law enforcement agencies must collaborate internationally to dismantle the infrastructure.
  - Utilize the [PhishDestroy free domain scanner](#) for domain verification.
  - Refer to the [DestroyList open-source blocklist](#) for known malicious domains.

## References

---

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

[Download IOCs \(CSV\)](#)

---

**PhishDestroy Research Division**

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

[phishdestroy.io](#) • [Free Scanner](#) • [DestroyList](#) • [ScamIntelLogs](#)

© 2019-2026 PhishDestroy. CC BY 4.0 • PD-MERCURYTEAM-2026-03-08